In the specification:

At page 1, lines 22-27:

Several particular watermarking techniques have been developed. The reader is presumed to be familiar with the literature in this field. Particular techniques for embedding and detecting imperceptible watermarks in media signals are detailed in the assignee's [~~co-pending application serial numbers 09/503,881 and 09/661,900, and~~] US Patent Nos. 6,122,403, 6,614,914 and 6,674,876, which are hereby incorporated by reference. In this document, we use the term "watermark" to refer to a digital watermark.

At page 5, lines 13-23:

Some practical facts that are important in many forensic tracking watermark applications can be learned from this example. Since the embedder is located in a consumer device, the embedder must be inexpensive. The embedder must also be real-time. Since the content owner owns the detector, it can be a powerful piece of equipment that can use a lot of time and processing power to find the watermark. In addition, since there is no interactivity requirements, such as required when using a content ID for interactive TV, the speed of detection and amount of content used to detect the watermark can be large. In forensic watermark detection, the whole piece of content, such as complete song, image or movie, is expected to be available, the detector has a greater opportunity to find the forensic watermark somewhere in the content. If the entire content is not available, [~~is~~] its value is degraded and is of less concern.

At page 6, lines 5-13:

At the broadcast side of the system, the broadcaster may optionally perform a watermark embedding operation 102 on the signal 100 to add a distributor identifier (ID) 104 according to an embedding protocol 106. The protocol specifies parameters of the digital watermark embedding operation, such as a carrier key used to modulate the message payload of the watermark, and a mapping key to map the message payload to features or samples of the host content signal. One example of carrier key is a pseudorandom number that acts as a carrier signal for the message payload. The message may modulate the carrier using a variety of

techniques, such as XOR, multiplication, convolution, phase shifting the carrier, adding shifted versions of the carrier together, etc.

At page 7, lines 5-8:

The broadcaster 108 distributes the content signal to two or more receivers 112, 212[~~, 224~~] (Receiver 1, 2, ... N) over a broadcast medium 110. This medium may be a conventional terrestrial broadcast carrier, a satellite broadcast, cable broadcast, Internet download or multicast, etc.

At page 10, lines 17-23:

Preferably, the embedders vary the forensic watermark from one device to another in a manner that reduces the effectiveness of averaging attacks. By using protocols and/or orientations that reduce interference between different forensic watermarks, the impact of averaging [~~to~~] copies of a content signal with different forensic watermarks is diminished. Certain aspects of the forensic watermark, such as the synchronization component may be similar for each copy, and therefore, averaging has little or no impact on it.

At page 11, lines 13-21:

Generational tracking can be enabled with standard non-variable embedding methods, by knowing or detecting the presence of a watermark layer and choosing a new watermark layer that has specifically been designed with a different non-interfering protocol. However, although this method is optimal in many situations, for many forensic tracking applications where the embedder is located in the consumer device, this method requires the embedder to also detect the watermark, thus increasing its cost. Even for server based forensic tracking embedders used in Internet streaming, the cost is a large requirement. To this end, the variable embedding approach enables generational forensic tracking at a reduced cost.

At page 12, lines 9-12:

As shown in block 308, the [~~The~~] first generation device then transfers the signal to some shared channel 124, such as portable memory device, networked storage location, etc.

Subsequent generations 310, 312 within different receivers perform the same functions to embed additional layers of forensic watermarks.

At page 12, lines 19-29:

In one implementation for video, the embedder employs a version of the embedding technique described in [~~co-pending application serial number 09/503,881 and~~] US Patent Nos. 6,122,403 and 6,614,914. The embedder generates an error correction encoded binary antipodal sequence corresponding to the forensic ID, spreads each bit of this sequence over a PN binary antipodal carrier key by multiplying each bit with the corresponding carrier key to form an intermediate signal, and maps elements of the intermediate signal to locations within selected blocks of the video. A perceptual analysis calculates data hiding capacity as a function of local spatial and temporal signal activity. This analysis produces a mask of gain values corresponding to locations with the host signal used to control embedding of the intermediate signal into the host signal. The gain values adjust the strength of the intermediate signal at the corresponding locations in the host signal.